Yee & Associates, P.C.

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner James A. Reagan Group Art Unit 3621**	Facsimile No.: **(571) 273-8300**
From: Stephanie Fay for Jennifer Pilcher Legal Assistant to Wayne Bailey	No. of Pages Including Cover Sheet: **43**
Message: Enclosed herewith: • Transmittal Document; and • Appeal Brief.	
Re: Application No. **09/598,777** Attorney Docket No: **00-022-MIS**	
Date: Monday, August 08, 2005	
Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.	*This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.*

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **McCown et al.**

Serial No.: **09/598,777**

Filed: **June 16, 2000**

For: **Method and System for Secure Credit Card Transactions**

§ Group Art Unit: **3621**
§
§ Examiner: **Reagan, James A.**
§
§ Attorney Docket No.: **00-022-MIS**
§

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on August 8, 2005.

By: Stephanie Fay

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37).

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to Storage Technology Corporation Deposit Account No. 19-4545. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to Storage Technology Corporation Deposit Account No. 19-4545. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to Storage Technology Corporation Deposit Account No. 19-4545.

Respectfully submitted,

Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEY FOR APPLICANTS

RECEIVED
CENTRAL FAX CENTER
AUG 08 2005

Docket No. 00-022-MIS

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **McCown et al.**	§	
Serial No. **09/598,777**	§	Group Art Unit: **3621**
Filed: **June 16, 2000**	§	Examiner: **Reagan, James A.**
For: **Method and System for Secure Credit Card Transactions**	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on August 8, 2005.

By: _____
Stephanie Fay

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on June 6, 2005.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

08/10/2005 EAREGAY1 00000003 194545 09598777
01 FC:1402 500.00 DA

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: Storage Technology Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-40

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: none
2. Claims withdrawn from consideration but not canceled: none
3. Claims pending: 1-40
4. Claims allowed: none
5. Claims rejected: 1-40
6. Claims objected to: none

C. CLAIMS ON APPEAL

The claims on appeal are: 1-40

STATUS OF AMENDMENTS

No amendment after final was filed for this case.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 - INDEPENDENT

Claim 1 is directed to a technique for improving security with respect to credit/debit card usage. A smart card having internal data processing capability is used to generate a unique billing digest that is transmitted by way of a merchant to a credit card issuing company. This unique billing digest – which is transmitted in addition to the usual transaction information such as customer information and merchant information – is compared with an independently generated authentication billing digest which is generated by the credit card issuer using information retrieved from a locally maintained database of customer information such that the authenticity of the transaction can be confirmed. A secret master key is used when generating the two digests, thus further enhancing the integrity of the transaction.

Specifically with respect to Claim 1, such claim is directed to a method for securing a transaction in order to prevent fraudulent transactions. Prior to the transaction, a secret master key is received from a third party, where the master key remains unchanged and is kept secret, and is not altered after the transaction. The third also stores a copy of this master key. A request for a digest is received from a requestor, and both the master key and unique client information are retrieved, the client information being associated with the master key. The digest is created by hashing (i) the unique client information and (ii) the master key. The (1) digest and (2) the unique client information (which was *also used* in creating the digest) are returned to the requestor, where the digest and the unique client information can then be used for transacting with the third party (Specification page 15, line 12 – page 18, line 18 with reference to Figures 3A-3B, all steps).

B. CLAIM 8 - INDEPENDENT

Claim 8 is directed to a method for securing a transaction in order to prevent fraudulent transactions. A smart card is initialized by receiving within the card a secret master key from a credit card issuer, the master key being kept secret. A data transmission from a merchant is received into the smart card, where the data transmission includes unique merchant information and a request for a billing digest. Unique client information is retrieved from the smart card

memory. The master key is retrieved. The billing digest is created by hashing the unique client information, the master key and the unique merchant information onboard the smart card. The billing digest, the unique merchant information and the unique client information are passed to the requestor (Specification page 15, line 12 – page 18, line 18 with reference to Figures 3A-3B, all steps).

C. CLAIM 11 - INDEPENDENT

Claim 11 is directed to a method for securing a transaction in order to prevent fraudulent transactions. A smart card is initialized by receiving within the card a secret master key from a credit card issuer, the master key being kept secret. A data transmission is sent to the smart card, where the data transmission includes unique merchant information and a request for a billing digest. The billing digest, the unique merchant information and unique client information is received from the smart card, the billing digest being hashed from the unique merchant information, unique client information and the master key from the smart card. The unique merchant information and unique client information is transmitted from the smart card to a credit card issuer (Specification page 15, line 12 – page 18, line 18 with reference to Figures 3A-3B, all steps).

D. CLAIM 13 - INDEPENDENT

Claim 13 is directed to a method for securing a transaction in order to prevent fraudulent transactions. Prior to the transaction, a secret master key is received from a third party, where the master key remains unchanged, and is not altered after the transaction, with the third party storing a copy of the master key within the third party, and the master key being kept secret. A third party receives a transaction request from a requestor, where the transaction request includes a digest and unique client information, the unique client information being associated with the master key. The copy of the master key is accessed based on the unique client information. An authorization digest is created by hashing the unique client information and the copy of the master key. The third party compares the authorization digest with the digest from the requestor, and returns a response to the requestor, the content of the response being based on an outcome of the comparison of the authorization digest with the digest from the requestor (Specification page 18, line 19 – page 20, line 23 with reference to Figures 4A-4B, all steps).

E. CLAIM 20 - INDEPENDENT

Claim 20 is directed to a method for securing a transaction in order to prevent fraudulent transactions. A billing digest is generated in a customer's smart card, the billing digest being hashed from merchant information, customer information and a secret master key. The master key is received from a credit card issuer upon an initialization of the smart card by the credit card issuer, the master key being associated with the customer information. An authentication digest is created by the credit card issuer, where the authentication digest is hashed from the merchant information, customer information and a master key associated with the customer information. The authorization digest is compared with the billing digest, and a transaction is authorized based on the comparison of the authorization digest with the billing digest (Specification page 15, line 12 – page 20, line 23 with reference to Figures 3A-3B and 4A-4B, all steps).

F. CLAIM 21 - INDEPENDENT

Claim 21 is directed to a method for securing a transaction. A secret master key is indexed to an account identifier for an account, where the account is between a customer and a financial institution. The master key is provided to the financial institution and a smart card controlled by the customer. Transaction data is passed through a third party, where the transaction data includes at least the customer account identifier, third party information and a billing digest which is created from the customer account identifier, the third party information and the master key (Specification page 13, line 8 – page 18, line 18; Figures 2 and 3A-3B, all elements).

G. CLAIM 22 - INDEPENDENT

Claim 22 is directed to a smart card for conducting secure transactions in order to prevent fraudulent transactions. The smart card comprises an input/output mechanism, a processor and a memory. The memory contains financial account information; a secret master key received upon initialization of the smart card, the master key remaining unchanged throughout the use of the smart card, the master key being received from a third party; a functional hashing algorithm; and an executable application for invoking the functional hashing algorithm, where the functional hashing algorithm creates a digest from the financial account information and the master key. The executable application transmits, via the input/output mechanism, the digest and the

financial account information to a requestor for approval by the third party (Specification page 11, line 15 – page 15, line 11).

H. CLAIM 23 - INDEPENDENT

Claim 23 is directed to a system for conducting secure transactions in order to prevent fraudulent transactions. The system comprises a client smart card for creating a billing digest from a resident client information, a resident secret master key and imported merchant information (the master key being received from a financial institution upon initialization of the smart card, the master key remaining unchanged after use of the smart card, the master key being kept secret, and the master key being associated with the resident client information); a merchant system for requesting the billing digest and for passing secure transaction information and the billing digest to the financial institution, wherein the transaction information comprises the client information, and the imported merchant information. The financial institution receives the transaction information and billing digest, and authorizes a transaction by (1) accessing a master key stored within the financial institution based on the client information, (2) creating an authorization digest from (i) the master key stored in the financial institution, the (ii) client information and (iii) the merchant information, and (3) comparing the authorization digest with the billing digest (Specification page 11, line 15 – page 20, line 23; Figures 2, 3A-B and 4A-B, all elements).

I. CLAIM 24 – INDEPENDENT

Claim 24 is a system claim of similar scope to Claim 1, and the summary of Claim 1 given above is equally applicable to Claim 24, and is thus hereby incorporated by reference. The structure for all of the listed means-for elements is provided by the functional blocks 210, 220 and 230 shown in Figure 2.

J. CLAIM 32 – INDEPENDENT

Claim 32 is a system claim of similar scope to Claim 13, and the summary of Claim 13 given above is equally applicable to Claim 32, and is thus hereby incorporated by reference. The structure for the receiving means, accessing means, creating means, comparing means and returning means are provided by block 140 shown in Figure 1.

K. CLAIM 39 – INDEPENDENT

Claim 39 is a program product claim of similar scope to Claim 1, and the summary of Claim 1 given above is equally applicable to Claim 39, and is thus hereby incorporated by reference.

L. CLAIM 40 – INDEPENDENT

Claim 40 is a program product claim of similar scope to Claim 8, and the summary of Claim 8 given above is equally applicable to Claim 40, and is thus hereby incorporated by reference.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1-3, 5-8, 10-14, 17-26, 28-33 and 36-40)

Claims 1-3, 5-8, 10-14, 17-26, 28-33 and 36-40 stand rejected under 35 U.S.C. § 103 as being unpatentable over Muftic (US 5,850,442 A), in view of Applicant's own admission, and further in view of Ranki, Smart Card Handbook © 1997.

B. GROUND OF REJECTION 2 (Claims 4, 9, 15-16, 27 and 34-35)

Claims 4, 9, 15-16, 27 and 34-35 stand rejected under 35 U.S.C. § 103 as being unpatentable over Muftic/Applicant/Ranki in view of Nguyen et al., (US Patent 5,931,917).

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-3, 5-8, 10-14, 17-26, 28-33 and 36-40)

A.1. Claims 1, 24 and 39

With respect to Claim 1 (and similarly for Claims 24 and 39), Appellants will first show that the Examiner's reasoning in combining the references and applying the teachings of such combination is logically inconsistent and therefore in error. Appellants will then show that even with such inconsistent reasoning, there are still missing claimed elements not taught or suggested by the cited references and thus the Examiner has failed to establish a prima facie showing of obviousness. If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

(i) Inconsistent Application of the Teachings of the Cited Muftic Reference re: Claim 1

In rejecting Claim 1, the Examiner makes the following statements regarding the teachings of Muftic:

(a) Muftic discloses "receiving, prior to the transaction, a secret *master key* from a third party... (see at least Abstract, Summary of the Invention, Fig 16: "smart token/certificate", associated text" (emphasis added by Appellants)

(b) Muftic discloses "retrieving the *master key* (retrieving unique client information)" (emphasis added by Appellants)

(c) "Although Muftic does disclose hashing a message digest, Muftic does not specifically disclose a *master key*" (emphasis added by Appellants)

Appellants show error in this analysis. First, Muftic's smart token/certificate is alleged to be the master key. Then, Muftic's unique client information is alleged to be the master key. Then, the Examiner acknowledges that Muftic does *not* disclose a master key. Appellants urge the last position (c) to in fact be the correct one – that Muftic does *not* disclose a master key.

This conclusion is evidenced by the fact that statement (a) cannot be true since the Muftic's smart token/certificate is stated to be the smart card itself (Muftic column 1, line 20;

column 10, lines 26-30), and there is no third party that stores a copy of the smart card. Claim 1 expressly requires that a copy of the master key (alleged by the Examiner to be the smart token, which per the teachings of Muftic is a smart card) is stored by a third party. Nor is statement (b), which equates "retrieving unique client information" to be the same as "retrieving the master key", correct. Muftic's unique client information is stated by the Examiner to be taught by Muftic's Figure 10 with respect to steps 1040 and 1060. Appellants urge that this Figure 10 and accompanying text describes a process for placing a customer order (column 13, lines 28-39). This unique client information is not received, prior to the transaction, from a third party as expressly recited in Claim 1 with respect to the claimed master key. Therefore, it is shown that an allegation that Muftic's unique client information reads on the claimed master key is incorrect. Thus, as allegations (a) and (b) are both erroneous, it logically follows – and as acknowledged by the Examiner – that Muftic 'does not specifically disclose a master key' (first full paragraph on page 4 of the present Office Action dated 9/22/2004).

Another inconsistency regarding the rejection of Claim 1 will now be shown. The Examiner states that Muftic teaches "creating the digest by hashing the unique client information and the master key (see at least C2, L38-41)". The Examiner then states in the next full paragraph "Muftic does not specifically disclose a master key, hashing a master key with customer information". These two statements are shown to be logically inconsistent, in that in the first instance it is alleged that the cited Muftic reference teaches *hashing unique client information and the master key*, and then in the second instance it is acknowledged that the cited Muftic reference does not disclose *hashing a master key with customer information*. In any event, Appellants urge that the passage cited by the Examiner as teaching hashing unique client information and a master key instead states the following (Muftic column 2, lines 38-41):

> "In modern implementations, a message digest is created using a cryptographically strong one way hash function based on the message text and the message digest operates like a CRC check sum."

Appellants urge that while this passage may make mention of creating a message digest using a one-way hash function that is based on a message text, such one-way hash function does not teach or otherwise suggest *hashing two items in the creation of a digest*, and in particular does

not teach or suggest "*creating the digest by hashing the unique client information and the master key*" (emphasis added by Appellants).

(ii) Claim 1 Missing Features

Specifically with respect to Claim 1, Appellants will now show that there are numerous claimed features not taught or suggested by any of the cited references. To establish prima facie obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03. *See also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974) (emphasis added by Appellants).

(a) There is no teaching or suggestion of the claimed master key (the master key being defined to be a key that remains unchanged and is kept secret, and is not altered after the transaction, the third party storing a copy of the master key) *that is used by a hashing operation.* As established above in the Inconsistent Application of the Cited Mustic Reference, Mustic does not teach or suggest the claimed master key that is used by a hashing operation. The cited Rankl reference also does not disclose any such master key that is used by a hashing operation. The Examiner alleges that Rankl clearly discloses hashing consumer data with the smart card unique key at Section 4.3 and Figure 4.23. Appellants urge that while the teaching in Section 4.3 is with respect to hashing, it describes a one-way hash function which derives a fixed-length value *from a variable-length document* (page 83, second paragraph in Section 4.3). There is no teaching or suggestion of any type of master key, either as a part of the hash function or otherwise. The cited figure at Figure 4.23 is with respect to *generation of a random number.* While this random number generation technique does appear to use a card specific key, there is no teaching, suggestion or other indication that this card specific key remains unchanged and is kept secret, is not altered after the transaction, with a third party storing a copy of this key, as expressly required by Claim 1. Still further, the use of this key is with respect to generation of a random number (as described by Rankl in Section 4.4), and *not with respect to any type of hashing operation.* Thus, it is shown that the cited Rankl reference similarly does not teach or suggest the use a master key, as defined in Claim 1, as a part of a hash function, as expressly required by Claim 1.

(b) None of the cited references teach or suggest the claimed step of creating a digest by hashing unique client information and the master key. Appellants have shown above in the

Inconsistence Application of the Mustic cited reference that Mustic does not teach or suggest this claimed step. *The cited Rankl similarly does not teach hashing two items – customer information and a master key – to create a digest.* Rather, it teaches (i) deriving a fixed length value from a variable length document (page 83, second paragraph in Section 4.3), and the use of a key to generate a random number (Figure 4.23). Thus, it has been shown that none of the cited references teach or suggest the claimed step of "creating the digest by hashing the unique client information and the master key".

(c) None of the cited references teach or suggest the claimed step of returning (i) the digest (*created by hashing* unique client information and a master key) and (ii) the unique client information (*used by the hashing process* to create the digest that is returned) to the requestor. The Examiner alleges that this step is taught by Muftic's Figure 10 and element 1060. Appellants urge that this cited passage merely teaches that a user digitally signs an order form and sends it to a server (column 13, lines 36-39). There is no teaching or suggestion that this step includes returning a digest that was created by hashing *unique client information* and a master key, *along with this same unique client information*, as expressly recited in Claim 1.

In conclusion regarding Claim 1, Appellants have shown numerous inconsistent interpretations per the teachings of the cited references. Appellants have further shown numerous claimed steps/features not taught or suggested by the cited references. As all of the claim limitations must be taught or suggested by the prior art in order to establish a prima facie showing of obviousness (MPEP 2143.03), it is shown that a prima facie case of obviousness has not been established with respect to Claim 1, and thus Claim 1 has been erroneously rejected by the Examiner.

A.2. Claims 2, 25 and 33

Appellants initially show error in the rejection of Claim 2 (and similarly for Claims 25 and 33) for reasons given above regarding Claim 1, of which Claim 2 depends upon.

Further with respect to Claim 2 (and similarly for Claims 25 and 33), Appellants urge that none of the cited references teach or suggest the claimed feature of "wherein the request further comprises unique requestor information and creating the digest further comprises hashing the unique requestor information". In rejecting Claim 2, the Examiner states that this is taught by Muflic's seller's ID shown in Figure 16. Appellants urge that this seller's ID (shown in Muflic's

Figure 16, box 1620) is described to be an electronic ID that a user fills in to electronic charge slip when making a purchase (Muflic column 14, lines 40-42). In contrast, the claimed unique requestor information as recited in Claim 2 is *a part of a request for a digest from a requestor.* In addition, Claim 2 goes on to state that as a part of creating this requested digest, *the unique requestor information is hashed.* Thus, information (seller's ID) that is received as part of the request from a requester for a digest is itself used in the creation of the digest. The teachings of Muflic are thus shown to be different for at least two reasons. First, the seller's ID is not part of a request for a digest from a requester, but is rather a manual user input value. Second, this seller's ID is not hashed when creating a digest. Thus, Claim 2 is further shown to not be obvious in view of the cited references as there are additional claimed features not taught or suggested by the cited references.

A.3. Claims 3 and 26

Appellants initially show error in the rejection of Claim 3 (and similarly for Claim 26) for reasons given above regarding Claim 1, of which Claim 3 depends upon.

Further with respect to Claim 3 (and similarly for Claim 26), Appellants urge that none of the cited references teach or suggest the claimed feature of "wherein the request includes unique merchant information which is used to access the master key". The Examiner acknowledges that the teachings of the cited Muflic reference are lacking in this regard, but states "it would have been obvious to one of ordinary skilled in the art at the time the invention was made to ensure that a request for billing digest would include unique merchant information that would dictate which master key the client system will fetch (i.e. Visa, MasterCard, AMEX, etc.). This would be inherent in the system, in order to allow it to properly match account holders and financial institutions". Appellants show twofold error in such assertion. First, inherency is not a proper basis for rejecting claims under 35 USC 103. Rather, inherency is a concept to be used in 35 USC 102 rejections[1]. Second, Claim 3 expressly states that the unique merchant information (included as a part of the digest request) is *used to access the master key.* None of the cited

[1] Under section 102(b), anticipation requires that the prior art reference disclose, either expressly or under the principles of inherency, every limitation of the claim. In re King, 801 F.2d at 1326, 231 USPQ at 138; RCA Corp. v. Applied Digital Data Sys., Inc., 730 F.2d 1440, 1444, 221 USPQ 385, 388 (Fed. Cir.), cert. dismissed, 468 U.S. 1228 (1984).

references teach or suggest such *use* of unique merchant information. Thus, Claim 3 is further shown to have been erroneously rejected as a prima facie showing of obviousness has not been established.

A.4. Claims 5, 28 and 36

Appellants initially show error in the rejection of Claim 5 (and similarly for Claims 28 and 36) for reasons given above regarding Claim 1, of which Claim 5 depends upon.

Further with respect to Claim 5 (and similarly for Claims 28 and 36), Appellants urge that none of the cited references teach or suggest the claimed feature of "wherein creating the digest by hashing is performed by a smart card", where the creation of the digest is defined to be "creating the digest by hashing the unique client information and the master key". In rejecting Claim 5, the Examiner states that this claimed feature is taught by Muflic at column 4, lines 33-43; and Muflic Figure 3 with associated text. Appellants show error in such assertion as follows. Muflic states at column 4, lines 33-43:

> "As advances in technology permit continued increases in the degree of miniaturization of electronic components, smart cards have been developed which include a processor and/or memory built into a transport medium the size of a typical credit card. The processors in these cards can be programmed like any other computer to perform desired functions. Smart card readers are known which permit one to both read the contents of a smart card, but also to interact with the smart card to change its contents and to accomplish cooperative functions which can range from the simple to the sophisticated."

Appellants urge that this generalized statement regarding advances in smart card technology does not teach or otherwise suggest *the specific features* of Claim 5, such as (i) creating a digest by a smart card, or (ii) hashing the unique client information and the master key by a smart card. As to Muflic's Figure 3 and associated text, Appellants urge that Muflic's Figure 3 does not even show a smart card or any associated operations that a smart card can perform. At best, it shows the existence of a smart card reader attached to a computer system. As to the text associated with Figure 3, such text states at column 10, lines 23-55:

"FIG. 3 is an illustration of a computer incorporating smart token hardware which can be used for running either client or server software.

In this exemplary illustration, the computer is equipped with the usual display 300, keyboard 330, mouse 340 and drives 320. *In addition, the computer is equipped with card reader 350 which will both read and write smart tokens such as smart cards or PCMCIA cards. Preferably, the cards are smart cards and card readers both read/write smart cards.* Although the term "reader" is used, it is to be understood that the term, as used herein, is intended to cover the writing of smart tokens as a necessary and inherent part of a "reader". Card reader 350 is illustrated as connected to the computer over cable 360 which connects to a port on the computer, such as an RS 232 port or via any other port or by a wireless connection.

Card readers may be external devices connected to computers, as illustrated in FIG. 1, or they may be built in to other devices such as CPU 310, telephones, vending machines, or almost any computer equipped device.

Although card reader 350 is equipped with a slot 370 for insertion of a smart card, smart card readers are also available which remotely sense the presence of a smart card in the vicinity of the reader and communicate with the smart card utilizing wireless technologies. In some such remote sensing card readers, the card readers broadcast an RF energy signal which is detected by the smart card and a response is sent from the smart card back to the remote sensing card reader. An interchange of data may then occur in both directions over the wireless link between the smart card and the reader. Some card readers are equipped with a keypad and display."

As can be seen, this passage merely describes an ability to read and write to a smart card, either by a reader or using RF wireless technology. There is no discussion of particular functionality that such a smart card performs, and in particular there is no teaching or suggestion of the *specific features* of Claim 5, such as (i) creating a digest by a smart card, or (ii) hashing the unique client information and the master key by a smart card. Thus, Claim 5 is further shown to have been erroneously rejected as there are further missing claimed features not taught or suggested by the cited references.

A.5. Claims 6 and 29

Appellants initially show error in the rejection of Claim 6 (and similarly for Claim 29) for reasons given above regarding Claim 1, of which Claim 6 depends upon.

Further with respect to Claims 6 (and similarly for Claim 29), Appellants urge that none of the cited references teach or suggest the claimed step of "encrypting the unique client information prior to retrieving the unique client information". The Examiner admits that this step is not taught by any of the cited references, but states that it would just be common sense to encrypt client information to prevent unauthorized access or capture. Appellants urge that such common sense basis for rejection under 35 USC 103 is contrary to judicial requirements in establishing obviousness: Although a device may be capable of being modified to run the way [the patent applicant's] apparatus is claimed, there must be a suggestion or motivation *in the reference* to do so. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990) (emphasis added by Appellants). Appellants urge that there is no such suggestion for encrypting the client information *prior to its retrieval*. The only suggestion for such encryption prior to retrieval comes from Appellants' own disclosure and claims, which is improper hindsight analysis. This can further be seen by Muflic's teaching of a user inputting information in an order form (Muflic Figure 10, box 1040), which is alleged by the Examiner to be equivalent to the claimed unique client information. It is not seen how user information that is manually entered in an electronic order form can be encrypted *prior to retrieving such user information*, as expressly recited in Claim 6. Thus, Claim 6 is further shown to have been erroneously rejected as there is at least one additional missing claimed step not taught or suggested by the cited references.

A.6. Claims 7, 30 and 38

Appellants initially show error in the rejection of Claim 7 (and similarly for Claims 30 and 38) for reasons given above regarding Claim 1, of which Claim 7 depends upon.

Further with respect to Claim 7 (and similarly for Claims 30 and 38), such claim recites further details of the unique requestor information recited in Claim 2. In rejecting Claim 7, the Examiner points to the teachings of Muftic at Figure 13 and the associated text. Appellants urge that Claim 7 recites that the details of the unique requestor information *are a part of the unique requestor information that is hashed* (per Claim 2) when creating the digest. The teachings associated with Muftic Figure 13 merely states that the seller exchanges the credit card slip for

the face amount less a service fee. Thus, the seller gets immediate cash (column 14, lines15-17). The teachings of Muftic do not teach or otherwise suggest the details of the unique requestor information recited in Claim 7, or the hashing of this information as a part of creating the digest. Thus, it is shown that Claim 7 is not obvious in view of the cited references as there are numerous claimed features not taught or suggested by such references.

A.7. Claims 8, 10 and 40

With respect to independent Claim 8 (and similarly for Claims 10 and 40), Appellants urge that none of the cited references teach or suggest (1) receiving, into the smart card, a data transmission from a merchant, wherein the data transmission includes unique merchant information, (2) creating a billing digest by hashing (i) unique client information, (ii) a master key and (iii) the unique merchant information onboard the smart card; or (3) passing (i) the billing digest, (ii) the unique merchant information and (iii) the unique client information to the requestor. In rejecting Claim 8, the Examiner relies upon the same reasoning given regarding Claim 1 in rejecting Claim 8. Appellants show that the Examiner has thus failed to establish a prima facie case of obviousness, as *Claim 8 recites additional features not recited in Claim 1.* Specifically, Claim 8 recites that a data transmission including *unique merchant information is received into a smart card.* Claim 1 is silent as to any type of merchant information, such as receiving such merchant information into a smart card. Claim 8 also recites that the billing digest is created by hashing unique merchant information onboard the smart card. Claim 1 is silent as to any type of merchant information, or operations pertaining thereto such as hashing unique merchant information onboard the smart card. Claim 8 also recites that the unique merchant information is passed to the requestor. Claim 1 is silent as to any type of merchant information, or operations pertaining thereto such as passing the unique merchant information to the requestor. Thus, it is shown that Claim 8 is of different scope than Claim 1, and therefore the Examiner has failed to establish a prima facie showing of obviousness with respect to Claim 8 by merely relying on the reasoning given in rejecting Claim 1. Accordingly, as a prima facie case of obviousness has not been established by the Examiner, the burden has not shifted to Appellants to rebut an obviousness assertion[2].

---

[2] In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie

A.8. Claims 11 and 12

With respect to independent Claim 11 (and dependent Claim 12), Appellants urge that none of the cited references teach or suggest the claimed steps of (1) sending a data transmission to a smart card, wherein the data transmission includes unique merchant information, (2) receiving unique merchant information from the smart card; or (3) transmitting the unique merchant information from the smart card to a credit card issuer. In rejecting Claim 11, the Examiner relies upon the same reasoning given regarding Claim 1 in rejecting Claim 11. Appellants show that the Examiner has thus failed to establish a prima facie case of obviousness, as *Claim 11 recites additional features not recited in Claim 1*. Specifically, Claim 11 recites that a data transmission that includes *unique merchant information is sent to a smart card.* Claim 1 is silent as to any type of merchant information, such as sending such merchant information to a smart card. Claim 11 also recites that unique merchant information is received from the smart card. Claim 1 is silent as to any type of merchant information, or operations pertaining thereto such as receiving unique merchant information from the smart card. Claim 11 also recites that the unique merchant information is transmitted from the smart card to a credit card issuer. Claim 1 is silent as to any type of merchant information, or operations pertaining thereto such as transmitting the unique merchant information from the smart card to a credit card issuer. Thus, it is shown that Claim 11 is of different scope than Claim 1, and therefore the Examiner has failed to establish a prima facie showing of obviousness with respect to Claim 11 by merely relying on the reasoning given in rejecting Claim 1. Accordingly, as a prima facie case of obviousness has not been established by the Examiner, the burden has not shifted to Appellants to rebut an obviousness assertion.

A.9. Claim 13, 18 and 32

With respect to independent Claim 13 (and similarly for Claims 18 and 32), Appellants urge that none of the cited references teach or suggest the claimed steps of (1) accessing the copy of the master key based on the unique client information, (2) creating an authorization digest by hashing the unique client information and the copy of the master key, or (3) comparing, by the third party, an authorization digest - that was created by hashing the unique client information

---

case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. Id.

and the copy of the master key - with the digest from the requestor. The cited Muftic reference merely teaches that authenticating an electronic message as to origin may involve validating a public key of a public key encryption pair of a user originating a message by using digital signatures of one or more certification authorities (column 7, lines 32-40). As this authentication technique is different from the transaction processing described in Claim 13, it similarly follows that the steps recited in Claim 13 are not inherent in the teachings of the cited Muftic reference[3]. Muftic also teaches checking the integrity of a document by generating a message digest of the document and appending the message digest to the document such that it can be compared to a message digest generated at the receiving end (column 2, lines 26-41). However, this process does not describe or otherwise contemplate any type of authorization digest that is created by hashing unique client information and the copy of the master key. Thus, Claim 13 is shown to not be obvious in view of the cited references as there are numerous claimed features not taught or suggested by such references.

A.10. Claim 14

Appellants initially show error in the rejection of Claim 14 for similar reasons to those given above with respect to Claim 13 (of which Claim 14 depends upon).

Further with respect to Claim 14, Appellants show additional error in the rejection of such claim for similar reasons to the further reasons given above with respect to Claim 2.

A.11. Claim 17

Appellants initially show error in the rejection of Claim 17 for similar reasons to those given above with respect to Claim 13 (of which Claim 17 depends upon).

Further with respect to Claim 17, Appellants show additional error in the rejection of such claim similar reasons to the further reasons given above with respect to Claim 5.

---

[3] "To establish inherency," the Federal Circuit recently stated, "the extrinsic evidence `must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill.'" *In re Robertson*, 169 F.3d 743, 745 [49 USPQ2d 1949] (Fed. Cir. 1999); see also *Continental Can Co. U.S.A., Inc. v. Monsanto Co.*, 948 F.2d 1264, 1268 [20 USPQ2d 1746] (Fed. Cir. 1991). Such inherency may not be established by "'probabilities or possibilities.'" *Continental Can*, 948 F.2d at 1269 (quoting In re Oelrich, 666 F.2d 578, 581 [212 USPQ 323] (C.C.P.A. 1981)).

A.12. Claim 19

Appellants initially show error in the rejection of Claim 19 for similar reasons to those given above with respect to Claim 13 (of which Claim 19 depends upon).

Further with respect to Claim 19, Appellants show additional error in the rejection of such claim for similar reasons to the further reasons given above with respect to Claim 7.

A.13. Claim 20

With respect to independent Claim 20, Appellants urge that none of the cited references teach or suggest the claimed step of "generating a billing digest in a customer's smart card, the billing digest being hashed from merchant information, customer information and a secret master key". As can be seen, this claimed step is directed to the generation of a billing digest, and such billing digest generation is done in a customer's smart card. In addition, this billing digest is hashed from three items - (i) merchant information, (ii) customer information and (iii) a secret master key. None of the cited references teach generation of a billing digest in a smart card, or that the billing digest is hashed from the three explicitly listed items of merchant information, customer information and a secret master key. Thus, it is shown that Claim 20 has been erroneously rejected as there are several missing claimed features not taught or suggested by the cited references.

A.14. Claim 21

With respect to independent Claim 21, Appellants urge that none of the cited references teach or suggest the claimed steps of (1) *indexing a secret master key to an account identifier for an account*, wherein the account is between a customer and a financial institution, or (2) passing transaction data through a third party, wherein the transaction data includes at least the customer account identifier, third party information and *a billing digest which is created from the customer account identifier, the third party information and the master key*. Nor has the Examiner alleged any such teaching or suggestion. Thus, a prima facie case of obviousness has not been established with respect to Claim 21, such claim has therefore been erroneously rejected.

A.15. Claim 22

With respect to independent Claim 22, such claim recites details of the smart card used for conducting secure transactions. None of the cited references teach or suggest a smart card that comprises (1) a functional hashing algorithm, and (2) an executable application for invoking the functional hashing algorithm, where the functional hashing algorithm creates a digest from (i) the financial account information and (ii) the master key. In addition, none of the cited references teach or suggest a smart card that transmits (i) this created digest and (ii) the financial account information to a requestor. Nor has the Examiner alleged any such teaching or suggestion. Thus, a prima facie case of obviousness has not been established with respect to Claim 22, and such claim has therefore been erroneously rejected.

A.16. Claim 23

With respect to independent Claim 23, none of the cited references teach or suggest the claimed features of (1) a client smart card for creating a billing digest from (i) a resident client information, (ii) a resident secret master key and (iii) imported merchant information; or (2) creating an authorization digest from (i) the master key stored in the financial institution, (ii) the client information and (iii) the merchant information. As to missing claimed feature (1), none of the cited references teach or suggest creating a billing digest by a smart card, the billing digest being created from, among other things, *imported merchant information*. As to missing claimed feature (2), none of the cited references teach or suggest using the three items expressly identified therein – a master key, client information, and merchant information – in creating an authorization digest that is used to compare against a billing digest. Therefore, it is shown that Claim 23 is not obvious in view of the cited references as there are numerous claimed features not taught or suggested by the cited references.

B. GROUND OF REJECTION 2 (Claims 4, 9, 15-16, 27 and 34-35)

B.1. Claims 4 and 27

Appellants show error in the rejection of Claims 4 and 27 for similar reasons to those given above with respect to Claim 1, and urge that the additional cited reference of Nguyen does overcome the teaching/suggestion deficiency described above with respect to Claim 1.

B.2. Claim 9

Appellants show error in the rejection of Claim 9 for similar reasons to those given above with respect to Claim 8, and urge that the additional cited reference of Nguyen does overcome the teaching/suggestion deficiency described above with respect to Claim 8.

B.3. Claims 15 and 34

Appellants show error in the rejection of Claims 15 and 34 for similar reasons to those given above with respect to Claim 13, and urge that the additional cited reference of Nguyen does overcome the teaching/suggestion deficiency described above with respect to Claim 13.

B.4. Claims 16 and 35

Appellants initially show error in the rejection of Claims 16 and 35 for similar reasons to those given above with respect to Claim 13, and urge that the additional cited reference of Nguyen does overcome the teaching/suggestion deficiency described above with respect to Claim 13.

Further with respect to Claims 16 and 35, Appellants show error in that none of the cited references teach or suggest the claimed features of "accessing all previously used reference numbers associated with the unique client information; comparing the previously used reference numbers with the reference number contained in the unique client information; and returning a response to the requestor, the content of the response being based on the outcome of the comparison of the previously used reference numbers with the reference number contained in the unique client information". Nor has the Examiner alleged any such teaching or suggestion. Thus, a prima facie case of obviousness has not been established with respect to Claims 16 and 35, and such claim has therefore been erroneously rejected.

In summary, there are numerous claimed features recited as a part of the method, system and program product of the present invention relating to secure transaction processing that are not taught or suggested by the cited reference, and thus as all of the claim limitations are not taught or suggested by the cited references, a prima facie case of obviousness has not been established as required by MPEP 2143.03, and such claims have therefore been erroneously rejected. In addition, as a prima facie case of obviousness has not been established, the burden has not shifted

to Appellants to rebut an obviousness assertion. It is therefore respectfully requested that the Board reverse the rejection of Claims 1-40.

Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

receiving, prior to the transaction, a secret master key from a third party, wherein the master key remains unchanged and is kept secret, and is not altered after the transaction, the third party storing a copy of the master key;

receiving a request for a digest from a requestor;

retrieving the master key;

retrieving unique client information;

the client information being associated with the master key;

creating the digest by hashing the unique client information and the master key; and

returning the digest and the unique client information to the requestor, wherein the digest and the unique client information will be used for transacting with the third party.

2. The method recited in claim 1 above, wherein the request further comprises unique requestor information and creating the digest further comprises hashing the unique requestor information.

3. The method recited in claim 1 above, wherein the request includes unique merchant information which is used to access the master key.

4. The method recited in claim 1 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

5. The method recited in claim 1 above, wherein creating the digest by hashing is performed by a smart card.

6. The method recited in claim 1 above further comprises encrypting the unique client information prior to retrieving the unique client information.

7. The method recited in claim 2 above, wherein the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, further wherein the unique requestor information includes information describing a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client.

8. A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

initializing a smart card by receiving within the card a secret master key from a credit card issuer, the master key being kept secret;

receiving, into the smart card, a data transmission from a merchant, wherein the data transmission includes unique merchant information, and a request for a billing digest;

retrieving unique client information, from the smart card memory;

retrieving the master key, the master key being known to the credit card issuer;

creating the billing digest by hashing the unique client information, the master key and the unique merchant information onboard the smart card; and

passing the billing digest, the unique merchant information and the unique client information to the requestor.

9. The method recited in claim 8 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the credit card issuer.

10. The method recited in claim 8 above further comprises encrypting the unique client information and the unique merchant information prior to passing the information to the merchant.

11. A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

initializing a smart card by receiving within the card a secret master key from a credit card issuer, the master key being kept secret;

sending a data transmission to the smart card, wherein the data transmission includes unique merchant information and a request for a billing digest;

receiving the billing digest, the unique merchant information and unique client information from the smart card, the billing digest being hashed from the unique merchant information, unique client information and the master key from the smart card; and

transmitting the unique merchant information and unique client information from the smart card to a credit card issuer.

12. The method recited in claim 11 above further comprises receiving a response from the credit card issuer.

13. A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

receiving, prior to the transaction, a secret master key from a third party, wherein the master key remains unchanged, and is not altered after the transaction, the third party storing a copy of the master key within the third party, the master key being kept secret;

receiving, by the third party, a transaction request from a requestor, wherein the transaction request includes a digest and unique client information, the unique client information being associated with the master key;

accessing the copy of the master key based on the unique client information;

creating an authorization digest by hashing the unique client information and the copy of the master key;

comparing, by the third party, the authorization digest with the digest from the requestor; and

returning a response to the requestor from the third party, the content of the response being based on an outcome of the comparison of the authorization digest with the digest from the requestor.

14. The method recited in claim 13 above, wherein the request includes unique requestor information and creating the authorization digest further comprises hashing the unique requestor information.

15. The method recited in claim 13 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

16. The method recited in claim 15 above further comprises:

accessing all previously used reference numbers associated with the unique client information;

comparing the previously used reference numbers with the reference number contained in the unique client information; and

returning a response to the requestor, the content of the response being based on the outcome of the comparison of the previously used reference numbers with the reference number contained in the unique client information.

17. The method recited in claim 13 above, wherein creating the authentication digest by hashing is performed by a smart card.

18. The method recited in claim 13 above further comprises decrypting the unique client information prior accessing the copy of the master key.

19. The method recited in claim 14 above, wherein the third party is a credit card issuer, the transaction is a credit card transaction and the requestor is a merchant, further wherein the requestor information includes information describing a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client.

20. A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

generating a billing digest in a customer's smart card, the billing digest being hashed from merchant information, customer information and a secret master key;

receiving the master key from a credit card issuer upon an initialization of the smart card by the credit card issuer, the master key being associated with the customer information;

creating an authentication digest by the credit card issuer, wherein the authentication digest is hashed from the merchant information, customer information and a master key associated with the customer information;

comparing the authorization digest with the billing digest; and

authorizing a transaction based on the comparison of the authorization digest with the billing digest.

21. A method for securing a transaction comprising:

indexing a secret master key to an account identifier for an account, wherein the account is between a customer and a financial institution;

providing the master key to the financial institution and a smart card controlled by the

customer;

passing transaction data through a third party, wherein the transaction data includes at least the customer account identifier, third party information and a billing digest which is created from the customer account identifier, the third party information and the master key.

22. A smart card for conducting secure transactions in order to prevent fraudulent transactions comprising:

a input/output mechanism;

a processor; and

a memory containing:

financial account information;

a secret master key received upon initialization of the smart card, the master key remaining unchanged throughout the use of the smart card, the master key being received from a third party;

functional hashing algorithm;

an executable application, for executing on the processor, for invoking the functional hashing algorithm, wherein the functional hashing algorithm creates a digest from the financial account information and the master key and further wherein the executable application transmits, via the input/output mechanism, the digest and the financial account information to a requestor for approval by the third party.

23. A system for conducting secure transactions in order to prevent fraudulent transactions comprising:

a client smart card for creating a billing digest from a resident client information, a resident secret master key and imported merchant information;

the master key being received from a financial institution upon initialization of the smart card, the master key remaining unchanged after use of the smart card, the master key being kept secret, and the master key being associated with the resident client information;

a merchant system for requesting the billing digest and for passing secure transaction information and the billing digest to the financial institution, wherein the transaction information comprises the client information, and the imported merchant information; and

the financial institution for receiving the transaction information and billing digest and for authorizing a transaction by:

accessing a master key stored within the financial institution based on the client information;

creating an authorization digest from the master key stored in the financial institution, the client information and the merchant information; and

comparing the authorization digest with the billing digest.

24. A system for securing a transaction in order to prevent fraudulent transactions comprising:

receiving means for receiving a secret master key from a third partition prior to the transaction, the master key remaining unchanged after the transaction, the master key being kept secret;

receiving means for receiving a request for a digest from a requestor;

retrieving means for retrieving the master key;

retrieving means for retrieving unique client information;

the client information being associated with the master key;

creating means for creating the digest by hashing the unique client information and the master key; and

returning means for returning the digest and the unique client information to the requestor, wherein the digest and the unique client information will be used for transacting with the third party.

25. The system recited in claim 24 above, wherein the request further comprises unique requestor information and creating the digest further comprises hashing the unique requestor information.

26. The system recited in claim 24 above, wherein the request includes unique merchant information which is used to access the master key.

27. The system recited in claim 24 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

28. The system recited in claim 24 above, wherein the creating means for creating the digest by hashing is performed by a smart card.

29. The system recited in claim 24 above further comprises encrypting means for encrypting the unique client information prior to returning the unique client information.

30. The system recited in claim 25 above, wherein the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, further wherein the unique requestor information includes information describing a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and transaction data which is specific to a transaction initiated by the client.

31. The system recited in claim 24 above further comprises:

fingerprint reading and identification means for reading a fingerprint and authorizing a client based on an identity of a client's fingerprint.

32. A system for securing a transaction in order to prevent fraudulent transactions comprising:

providing means for providing from a third party a secret master key to a client, the master key remaining unchanged after the transaction;

receiving means for receiving a transaction request from a requestor, wherein the transaction request includes a digest and unique client information, the digest being created utilizing the master key provided to the client and the unique client information, the unique client information being associated with the master key;

accessing means for accessing, by the third party, a master key stored within the third party based on the unique client information;

creating means for creating an authorization digest by hashing the unique client information and the master key;

comparing means for comparing the authorization digest with the digest from the requestor; and

returning means for returning a response to the requestor, the content of the response being based on the outcome of the comparison of the authorization digest with the digest from the requestor.

33. The system recited in claim 32 above, wherein the request includes unique requestor information and creating the authorization digest further comprises hashing the unique requestor information.

34. The system recited in claim 32 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

35. The system recited in claim 34 above further comprises:

accessing means for accessing all previously used reference numbers associated with the unique client information;

comparing means for comparing the previously used reference numbers with the reference number contained in the unique client information; and

returning means for returning a response to the requestor, the content of the response being based on the outcome of the comparison of the previously used reference numbers with the

reference number contained in the unique client information.

36. The system recited in claim 32 above, wherein creating the authentication digest by hashing is performed by a smart card.

37. The system recited in claim 32 above further comprises decrypting the unique client information prior accessing the copy of the master key.

38. The system recited in claim 33 above, wherein the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, further wherein the requestor information includes information describing a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and transaction data which is specific to a transaction initiated by the client.

39. A computer program product for securing a transaction in order to prevent fraudulent transactions embodied on a computer readable medium comprising:

providing instructions for providing from a third party a secret master key, the master key remaining unchanged after the transaction;

receiving instructions for receiving a request for a digest from a requestor;

retrieving instructions for retrieving the master key;

retrieving instructions for retrieving unique client information;

the master key being associated with the client information;

creating instructions for creating the digest by hashing the unique client information and

the master key; and

returning instructions for returning the digest and the unique client information to the requestor, wherein the digest and the unique client information will be used for transacting with the third party.

40. A computer program product for securing a transaction in order to prevent fraudulent transactions embodied on a computer readable medium comprising:

initializing instructions for initializing a smart card by receiving within the card a secret master key from a credit card issuer;

receiving instructions for receiving, into the smart card, a data transmission from a merchant, wherein the data transmission includes unique merchant information, and a request for a billing digest;

retrieving instructions for retrieving unique client information, from the smart card memory;

the unique client information being associated with the master key;

retrieving instructions for retrieving the master key, the master key being provided by the credit card issuer;

creating instructions for creating the billing digest by hashing the unique client information, the master key and the unique merchant information onboard the smart card; and

passing instructions for passing the billing digest, the unique merchant information and the unique client information to the requestor.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.